CORE COMPLIANCE & LEGAL SERVICES, INC.
SOLUTIONS FOR TODAY'S BUSINESS

Risk Management Update
October 2012

CLOUD COMPUTING CONSIDERATIONS FOR FINANCIAL FIRMS

As more and more firms are using Cloud based computing to back up and store their electronic records, it is important that firms fully understand how this service actually works and the risks involved with this increasingly popular service offering. Cloud computing is still evolving, making security an ongoing challenge for service providers as well as the firms using this technology.

What is "the cloud?" The cloud refers to the infrastructure, applications, and business processes that can be delivered to your firm as a service over the internet or your own network. There are public, private and hybrid cloud virtual data centers. The cloud providers manage the infrastructure and platforms on which the applications run. End users can access cloud based applications through a web browser, while the business software and user's data are stored on servers in remote locations.

Proponents claim cloud computing gives firms the ability to get their applications up and running faster, which improves manageability and requires less maintenance. The IT Department is able to make adjustments more quickly to ever changing business demands, allowing firms to gain access to new services while reducing capital expenditures. Another benefit is the ease of procuring the service without going through the lengthy IT process of implementing it in house. Firms are able to try new applications and integrate new capabilities without first investing in expensive equipment that they may not need in the long run.

In addition to these benefits, there are also some challenges. These include the loss of control over your data, vulnerabilities to the strength and performance of the service provider, inherent challenges in testing and maintaining compliance with industry standards, safeguarding data locations, barriers between data storage of multiple clients, security of the facilities running the service and storing the data, and accessibility to your data.

Consequently, you need to fully understand the service, related regulatory considerations, the safeguards in place to protect your data from attack, and the ease of accessing your data. It is important for firms to visit these facilities to see first-hand the safeguards in place for data integrity and protection. Performing on-going due diligence will be one of the most fundamental requirements you will face in managing this service.

How to Prepare For Cloud Based Computing

Before you get started it is important to understand every stage of the process to fully understand the risks associated with the Cloud and to prepare for effectively testing the process. In the initial

phase, you will need to transfer the data to the service provider. Next, you will need to work with the provider to understand the process for encrypting, storing, disaster protection and recovery.

Understanding Your Options

Generally there are three basic options for financial firms:

1. A fully managed environment where a third party manages the facility, hardware and storage;
2. Co-locations using your own equipment storage but someone else's facility, whereby you manage your equipment, they manage the facility; or
3. A hybrid model where you buy your own equipment and use someone else's backup facility and they actually manage it.

Once you select the appropriate model for your business, you should look at several service providers and request proposals from each. Typically there is commonality in their pricing models; you are charged based on how much space you use, by the power that is metered or charged by capacity. You also should evaluate the experience of the provider to ascertain if there is a difference in quality of the power grids and of the employees. Generally, the larger the firm the more costly it will probably be for the service. Smaller cloud service provider firms seem more interested in building long-term relationships. In addition, look at where your data is being stored and assess whether all equipment and storage is in a shared environment. If so, you will need to further investigate how your data will be safeguarded and protected.

Final Tips from Users

1. It is difficult to manage infrastructure and platforms with third party vendors.
2. Cost over time may increase. The high cost of building and managing these locations may slowly cause your fees to escalate. Some have found they get a good deal to start for the first few years, then later as their contract renews the costs start to increase.
3. The quality of the people counts. There are not enough experts in cloud computing which should give you pause if you are allowing someone else to manage your confidential data.

How to Protect Yourself

Safeguard considerations are paramount; consider the following when evaluating a potential service provider:

1. Perform due diligence.
2. Evaluate vendor safeguards, particularly in shared environments. This will protect your data from being manipulated or stolen.
3. Ensure that the network is segregated. If a hacker gains access to a non-segregated system, all information is stolen, including yours.

4. Evaluate the sophistication of the vendor. You need to be diligent when looking at a smaller firm looking to grow to ensure they have the systems in place to protect your data.

For more information or to learn how Core Compliance & Legal Services, Inc. may be of assistance, please do not hesitate to contact us at (619) 278-0020.

Author: Sandy Pappalardo, Sr. Compliance Consultant; Editor: Michelle L. Jacko, CEO, Core Compliance & Legal Services ("CCLS"). CCLS works extensively with investment advisers, broker-dealers, investment companies, hedge funds, private equity firms and banks on regulatory compliance issues. For more information about this topic and other compliance consultation services, please contact us at (619) 278-0020, info@corecls.com or visit www.corecls.com.